

In order to answer the questions below use your self created lecture notes, sections of text book (s) read, library databases and/or the Internet can be used to answer the questions. But reference all information accordingly.

Protecting Functionality

1. Discuss the fact that general management, IT management, and information security management are responsible for implementing information security to protect the ability of the organization to function.

Protecting Data that Organizations Collect and Use

1. Explain data security, as it relates to protecting data in motion and data at rest.

Enabling the Safe Operation of Applications

1. Discuss that today's organizations are under immense pressure to create and operate integrated, efficient, and capable applications. The modern organization needs to create an environment that safeguards applications using the organization's IT systems, particularly those applications that serve as important elements of the organization's infrastructure.

Threats and Attacks

1. Explain threat and point out that an attack represents an ongoing act against the asset that could result in a loss. Do threat agents use exploits to take advantage of vulnerabilities where controls are not present or are no longer effective?

Compromises to Intellectual Property

1. Explain intellectual property (IP) and is included for an organisation IP.

Copyright Protection and User Registration

1. Discuss enforcement of copyright laws and a number of technical security mechanisms, such as digital watermarks, embedded code, and copyright codes.

Hackers

1. Discuss the act of trespassing which can lead to unauthorized, real, or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.
2. Discuss the classic perpetrator of deliberate acts of espionage or trespass as a hacker. In the gritty world of reality, a hacker uses skill, guile, or fraud to attempt to bypass the controls placed around information that is the property of someone else. Hacker frequently spends long hours examining the types and structures of the targeted systems.
3. Explain who is an expert hacker
4. Discuss the term privilege escalation. Would you consider jailbreaking or rooting examples of privilege escalation? Give your reason whether it is yes or no.

Hacker Variants

1. Explain the following terms:
 - Cracker
 - A phreaker

Password Attacks

1. Discuss these four approaches to password cracking:
 - Brute force
 - Dictionary attacks
 - Rainbow tables
 - Social engineering password attacks

Forces of Nature

1. Discuss how forces of nature, *force majeure*, or acts of God pose some of the most dangerous threats, because they are unexpected and can occur with very little warning.
2. Discuss the following examples of force of nature threats:
 - a. Fire
 - b. Flood
 - c. Earthquake
 - d. Lightning
 - e. Landslides or mudslides
 - f. Tornados or severe windstorms
 - g. Hurricanes, typhoons, and tropical depressions
 - h. Tsunamis
 - i. Electrostatic discharge (ESD)
 - j. Dust contamination
 - k. Solar activity

Explain the following terms and give examples or outline a scenario:

- Human Error or Failure
- Social Engineering
- Information Extortion
- Sabotage or Vandalism
- Software Attacks
- Malware
- *Virus*
- *Worms*
- *Trojan Horses*
- *Polymorphic Threats*
- *Virus and Worm Hoaxes*
- Back Doors
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- E-mail Attacks
- Communications Interception Attacks
- *Packet Sniffer*
- *Spoofing*
- *Pharming*
- *Man-in-the-Middle*

The OWASP Top 10

1. Discuss the Open Web Application Security Project (OWASP) that was founded in 2001 as a nonprofit consortium.

Threats and Attacks

1. What is the difference between a threat and an attack?

Useful Resources

1. Cross-site scripting FAQ
<http://www.cgisecurity.com/xss-faq.html>
2. Governing for Enterprise Security Implementation Guide
<http://www.cert.org/governance/ges-xteam.html>
3. Build Security In: Secure Software Development Lifecycle
<https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/sdlc/326-BSI.html>
4. Build Security In: Making the Case for Software Assurance
<https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/685-BSI.html>
5. Verizon Data Breach Investigations Report (2016)
www.verizonenterprise.com/verizon-insights-lab/dbir/2016
6. NIST 800-100
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf>